REMARKS

The present application was filed on July 31, 2003 with claims 1-30. Claims 1-30 are currently pending in the application. Claims 1 and 28-30 are the independent claims.

Claims 1-30 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 7,082,604 (hereinafter "Schneiderman").

In this response, Applicants traverse the §102(e) rejection, and submit a Notice of Appeal. It is expected that the Notice of Appeal will be followed in due course by an Appeal Brief.

Applicants respectfully request reconsideration of the present application in view of the remarks below.

With regard to the §102(e) rejection of claims 1-30, Applicants respectfully traverse. Applicants initially note that MPEP §2131 specifies that a given claim is anticipated "only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference," citing Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, MPEP §2131 further indicates that the cited reference must show the "identical invention . . . in as complete detail as is contained in the . . . claim," citing Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

Independent claim 1 is directed to a method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device. The method includes the steps of associating a given set of nodes of a graph characterizing the cryptographic functionality with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes. The recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality.

In an illustrative embodiment, cryptographic functionality is partitioned to permit delegation of at least one of a number of different distinct portions of the cryptographic functionality from a

delegating device 102D to at least one recipient device 104R. See FIG. 1 of the drawings. A given set of nodes of a graph is associated with a corresponding one of the distinct portions of the cryptographic functionality. The nodes of the graph in the illustrative embodiment correspond generally to seeds arranged in different levels as shown, for example, in FIG. 4. See the specification at page 6, lines 8-18. As shown in the flow diagram 300 of FIG. 3, the delegating device 102D in step 302 transmits one or more seeds associated with a particular portion of the partitioned cryptographic functionality to the recipient device 104R. In step 304, the recipient device 104R utilizes the transmitted seed or seeds to compute one or more additional seeds which permit authorized execution of the particular portion of the partitioned cryptographic functionality by the recipient device 104R.

Advantageously, such an approach ensures that the recipient device 104R cannot execute the particular portion of the cryptographic functionality until it receives the appropriate transmitted seeds. See the specification at page 6, lines 26-28. More generally, by characterizing cryptographic functionality as a graph, and associating a given set of nodes of the graph with a corresponding one of a plurality of distinct partitioned portions of the cryptographic functionality, the claimed arrangements overcome the significant problems associated with the conventional identity-based encryption (IBE) approach described at page 1, line 18-24.

The Examiner argues that the Schneiderman reference teaches each and every one of the above-noted limitations of claim 1. Applicants respectfully disagree. In formulating the rejection of claim 1, the Examiner relies on FIGS. 24-25 and column 1, lines 10-31, column 3, lines 49-67, column 21, lines 54-67, and column 22, lines 10-48. See the final Office Action at page 4, last paragraph. However, the relied-upon portions of Schneiderman fail to meet the limitations of claim 1. For example, these portions of Schneiderman fail to teach or suggest the recited step of associating a given set of nodes of a graph characterizing cryptographic functionality with a corresponding one of a plurality of distinct portions of the cryptographic functionality. The tree node data model of Schneiderman as described in the relied-upon portions is not representative of partitioned cryptographic functionality as in the claimed arrangement, but instead is a tree model of running servers and agents. See Schneiderman at column 22, lines 10-11. The nodes of the

Schneiderman tree model are thus associated with particular servers and agents, and not with respective distinct portions of any particular cryptographic functionality.

The Examiner in the final Office Action further argues that the Field of Invention in column 1 of Schneiderman provides additional support for the anticipation rejection of claim 1. However, the Field of Invention, like the rest of the Schneiderman reference, provides no teachings whatsoever regarding the recited partitioning of cryptographic functionality. In fact, the entirety of the Schneiderman reference fails to even mention cryptographic functionality, much less the partitioning of cryptographic functionality in a manner that associates a given set of nodes of a graph with a particular one of a plurality of distinct portions of the partitioned cryptographic functionality as recited in claim 1.

The Field of Invention portion of Schneiderman, and the other relied-upon portions, relate to distributing computing arrangements in which computing tasks are broken down into smaller tasks and distributed for simultaneous execution by mobile agents. Such teachings fail to anticipate the claimed arrangement which requires association of a given set of nodes of a graph characterizing cryptographic functionality with a corresponding one of a plurality of distinct partitioned portions of the cryptographic functionality, along with transmission of information representative of the nodes from a delegating device to a recipient device. Moreover, such teachings fail to provide the advantages of the claimed arrangements in terms of overcoming the problems associated with the conventional IBE approach.

The Examiner also appears to argue that FIG. 10 of Schneiderman relates to cryptographic functionality because it refers to "keys of a hash table." See the final Office Action at page 3, second paragraph. However, the hash table does not relate to cryptographic functionality, but instead to a storage element that simply stores "references to the actual agent threads that are running on the server machine." The keys of the hash table are not cryptographic keys, but are instead expressly described as simply indicating "the names of the running agents." See Schneiderman at column 14, lines 52-56. Thus, the keys and hash table in Schneiderman merely relate to a storage and lookup mechanism for keeping track of what agents are running on a given server. Such teachings do not relate in any way to cryptographic functionality, much less the recited

graph-based partitioning of cryptographic functionality set forth in claim 1. To the contrary, it appears that the Schneiderman arrangements relied upon by the Examiner do not involve the performance of any type of cryptographic functionality.

Accordingly, it is believed that Schneiderman fails to meet the limitations of independent claim 1. The anticipation rejection should therefore be withdrawn.

Dependent claims 2-27 are believed allowable for the reasons outlined above with regard to claim 1, and are also believed to define separately patentable subject matter relative to Schneiderman.

For example, dependent claim 2 indicates that the at least one of the nodes of the graph corresponds to a seed, where the possession of that seed permits execution of a corresponding one of the distinct portions of the cryptographic functionality. The Examiner argues that this limitation is met by the teachings in column 21, lines 54-67, of Schneiderman. See the final Office Action at page 5, first paragraph. However, the relied-upon portion of Schneiderman makes no mention whatsoever of seeds, but instead indicates that tree nodes correspond to servers. The limitations of claim 2 are clearly not met by this portion of Schneiderman. Furthermore, as noted above, the "keys of a hash table" referred to in the context of FIG. 10 of Schneiderman do not relate to cryptographic keys or other cryptographic functionality, but instead simply provide "the names of the running agents" for a particular server. The limitations of claim 2 are therefore clearly not met by the Schneiderman reference.

As another example, dependent claim 9 states that the graph comprises L levels of nodes, an Lth one of the levels comprising a parent node $v_{L,1}$, and a first one of these levels comprising a set of seeds $v_{1,1}, v_{1,2}, \ldots v_{1,n}$, where n is the total number of seeds, each of the seeds being derivable from the parent node. An example of such an arrangement is shown in FIG. 4 of the drawings in the present application. The Examiner argues that each and every one of these limitations is met by Schneiderman, relying on FIGS. 24-25, column 1, lines 10-31, and column 3, lines 49-67. See the final Office Action at page 6, second paragraph. Again, the relied upon portions do not even mention seeds, much less the particular recited arrangement of a graph in which particular levels comprise particular seeds.

Additional examples can be seen in dependent claims 10, 11 and 12, which further limit the particular graph structure of claim 9. Again, the Examiner argues that these limitations are anticipated by portions of Schneiderman, namely FIGS. 24-25, column 1, lines 10-31, and column 3, lines 49-67, which do not even mention seeds, or the association of particular seeds with particular levels of a graph.

Still further examples of the fundamental deficiency of the anticipation rejection over Schneiderman can be seen with reference to dependent claims 13-16, which recite "a hardware-based authentication token." An example of such a token is described in the specification at page 14, lines 20-25. The Examiner argues that the hardware-based authentication token limitations of claims 13-16 are met by the teachings in column 3, lines 7-67, of Schneiderman. See the final Office Action at page 6, last two paragraphs, to page 7, first two paragraphs. However, there is no mention or suggestion whatsoever in these relied-upon passages, or elsewhere in Schneiderman, regarding hardware-based authentication tokens, much less the particular limitations involving such tokens that are set forth in claims 13-16.

Similarly, Schneiderman fails to disclose or suggest the generation and verification of signatures as set forth in claim 17, generation of values of a one-way chain as set forth in claim 18, the performance of symmetric or asymmetric cryptographic operations as set forth in claim 19 and 20, the derivation of one or more cryptographic keys as set forth in claim 21, the computation of one or more seeds as set forth in claims 22 and 23, or the partitioning of cryptographic functionality in accordance with a subscription model as in claims 24 and 25. The particular portions of the Schneiderman reference relied upon as being allegedly anticipatory of each of these features clearly fail to teach or suggest the features in question. For example, as noted previously, the "keys of a hash table" mentioned in the context of FIG. 10 of Schneiderman are not seeds or cryptographic keys, but are instead just "the names of the running agents" on a particular server. These values have nothing whatsoever to do with cryptographic functionality, partitioned or otherwise.

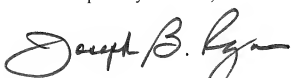
The §102(e) rejection is similarly deficient with regard to the other dependent claims.

Independent claims 28-30 are believed allowable for reasons similar to those outlined above with regard to claim 1.

In view of the foregoing, claims 1-30 are believed to be in condition for allowance.

As indicated previously, a Notice of Appeal is submitted concurrently herewith.

Respectfully submitted,



Date: January 2, 2008

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

Enclosure(s): Notice of Appeal